UK Patent Application (19) GB (11) 2 193 867 (13) A

(43) Application published **17 Feb 1988**

(21) Application No **8625487**

(22) Date of filing **24 Oct 1986**

(30) Priority data
(31) **8619737**   (32) **13 Aug 1986**   (33) **GB**

(71) Applicants
Philips Electronic and Associated Industries Limited

(Incorporated in United Kingdom)

Arundel Great Court, 8 Arundel Street, London WC2R 3DT.

Direct Broadcasting Limited

(Incorporated in United Kingdom)

Kensington Business Centre, 9/11 Kensington High Street, London W8 5NP

(51) INT CL⁴
H04N 7/16 H04K 1/00

(52) Domestic classification (Edition J):
H4R 17D 17V 22V CST PTS
H4F D13A D1A9 D22 D30K DE

(56) Documents cited
EP A 0053885   WO 83/04154

(58) Field of search
H4R
H4F
Selected US specifications from IPC sub-classes H04K
H04N

(72) Inventors
Gerald Offley Crowther
Peter Robert Brennand

(74) Agent and/or Address for Service
R. J. Boxall,
Mullard House, Torrington Place, London WC1E 7HD

(54) **Decoding transmitted scrambled signals in a pay television system**

(57) In a pay television system a programme signal is transmitted scrambled to prevent its un-authorised reception, the scrambled signal being accompanied by authorisation codes, one for each authorised subscriber, a subscription key and a pay-per-view key. At a receiver if the appropriate authorisation code is received the receiver functions in the subscription mode in which mode the subscription key provides for the descrambling of the programme signal. If the appropriate authorisation code is not received indicating that the subscriber is not pre-authorised to receive the programme in an inelligible manner, the receiver is set to function in a pay-per-view mode in which mode, on request, the pay-per-view key provides for the descrambling of the programme signal. Details of message packets and the encryption are disclosed.

GB 2 193 867 A

The drawings originally filed were informal and the print here reproduced is taken from a later filed formal copy.
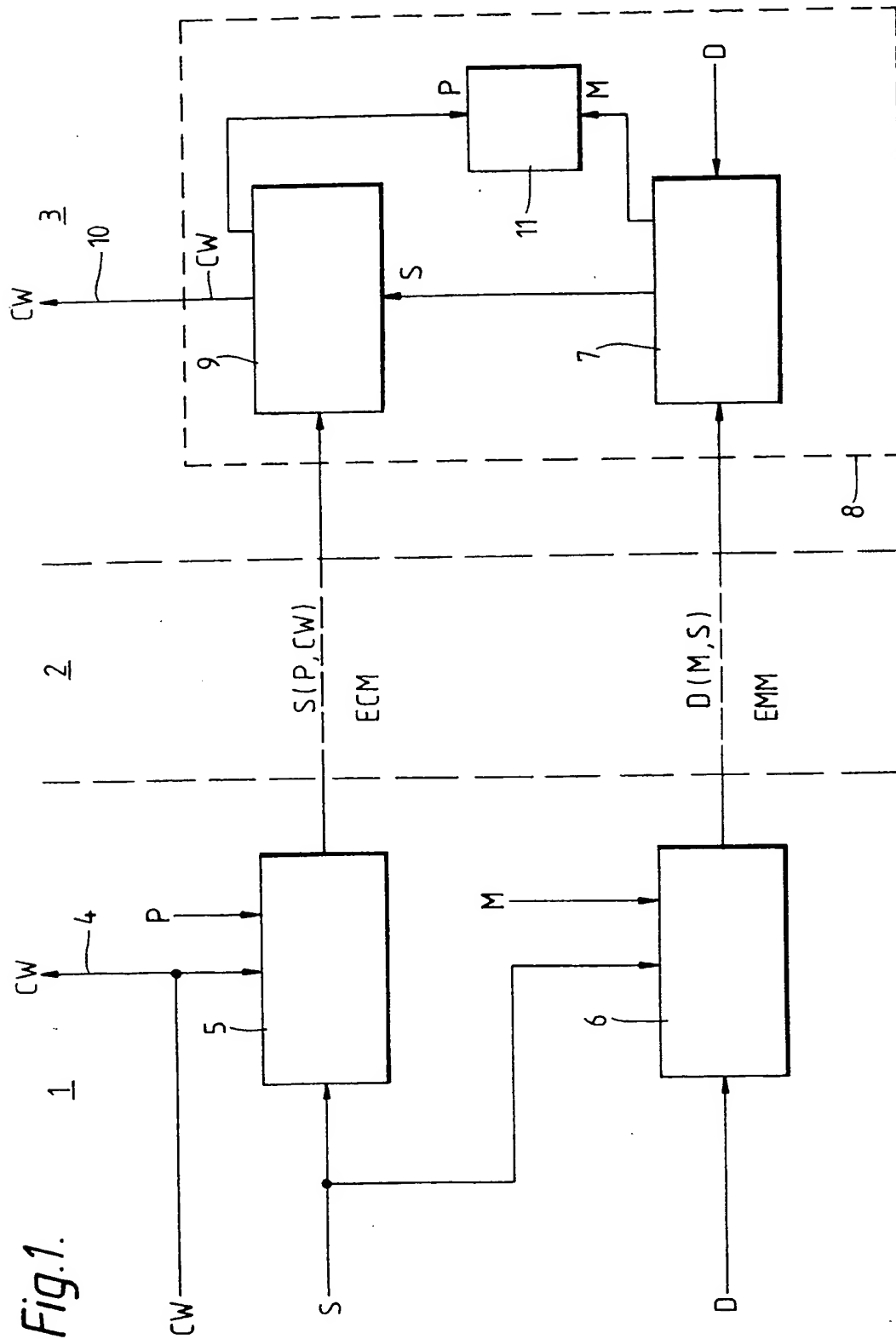
Fig.1.

2193867

Fig.2.

PH	PT	UCA	UCBMD	U	SDKUP	SAUP	CPUP	CTUP		
23	8	(36)	(4)	(64)	(64)	(48)	(10)	(12)	(118)	(4)

Fig.3.

PH	PT	SCA	VALMD	Spn	276 × 1 bit
23	8	(24)	(4)	(56)	(276)

Fig.4.

PH	PT	CI	LI	PI	LI	SKL	P A S E M M	P A S E C M	Spn (Spc)	PI	LI	Spc	CW	P C A T	C H I D	P N U M	PI	PPV PR 5 bytes
		00	81	00	25					02 or 03	48							
23	8	(8)	(8)	(8)	(8)	(12)	(12)	(12)	(64)	(8)	(8)	(56)	(64)	(8)	(16)	(24)	(8)	(16) 40

Fig.5.

BYTE 1	BYTE 2	BYTE 3	BYTE 4	BYTE 5	BYTE 6	BYTE 7	BYTE 8

B0	B1	B2	B3

2193867
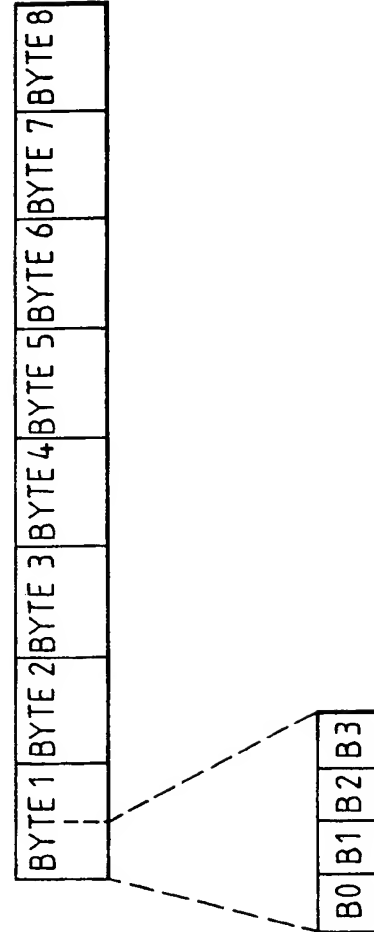
Fig.6.

PH	PT	SCA	VALMD	Ssc	CA
					276 × 1 bit
23	8	(24)	(4)	(56)	(276)

Fig.7.

PH	PT	CI	LI	PI	LI	PL	PI	LI	Ssc	CW	PCAT	CHID	PNUM	PI	30 bytes
		01	56	01	4		04	44							
23	8	(8)	(8)	(8)	(8)	(16)	(8)	(8)	(56)	(64)	(8)	(16)	(24)	(8)	240

2193867

Fig. 8.

Fig.9A.

2193867

Fig.9B.

F16
FIA?
N
F18
CHG
Y

SUP CW   F17

F19
EMM & ECM = 0
Y   N

F22
SCH SUB EMM

F23
WT SUB EMM

F24
US AUTH?
N   Y

F25
SCH PR EMM

F26
OB Ssc

F20
WT PR ECM

F21
MON PR ECM

F14

F27

7 -IX- PHB 33290 R

2193867

Fig.9C.

```
                         ┌──────────────┐ F27
                         │              │
                         │  SCH PR EMM  │
                         │              │
                         └──────┬───────┘
                         ┌──────┴───────┐ F28
                         │              │
                         │  SCH SUB ECM │
                         │              │
                         └──────┬───────┘
              ┌─────────►┌──────┴───────┐ F29
              │          │  WT  SUB ECM │
              │          └──────┬───────┘
              │                 │
              │            ╱────┴────╲ F30
              │           ╱           ╲         Y
              │          ╱   PL CH?    ╲──────────────►┌──────────────┐ F31
              │          ╲             ╱               │              │
              │           ╲           ╱                │  SCH PR ECM  │
              │            ╲────┬────╲                 │              │
              │              N  │                      └──────┬───────┘
              └─────────────────┘                     ┌───────┴──────┐ F32
                                                      │  WT PR ECM   │
                                                      └───────┬──────┘
                                                      ┌───────┴──────┐ F33
                                                      │              │
                                                      │   OBT Spn    │
                                                      │              │
                                                      └───────┬──────┘
                                                        F14   │
                                                              ▼
```

2193867
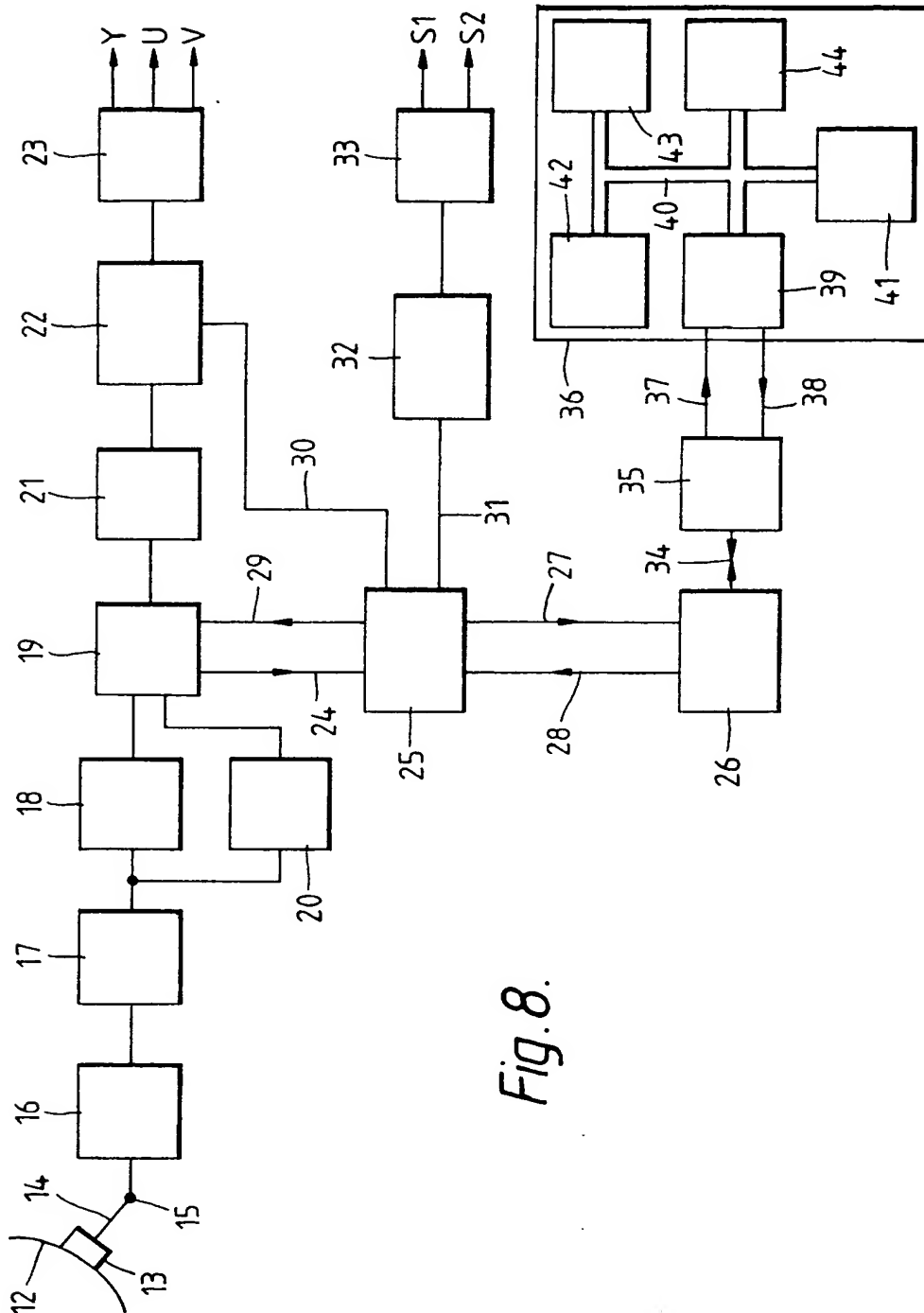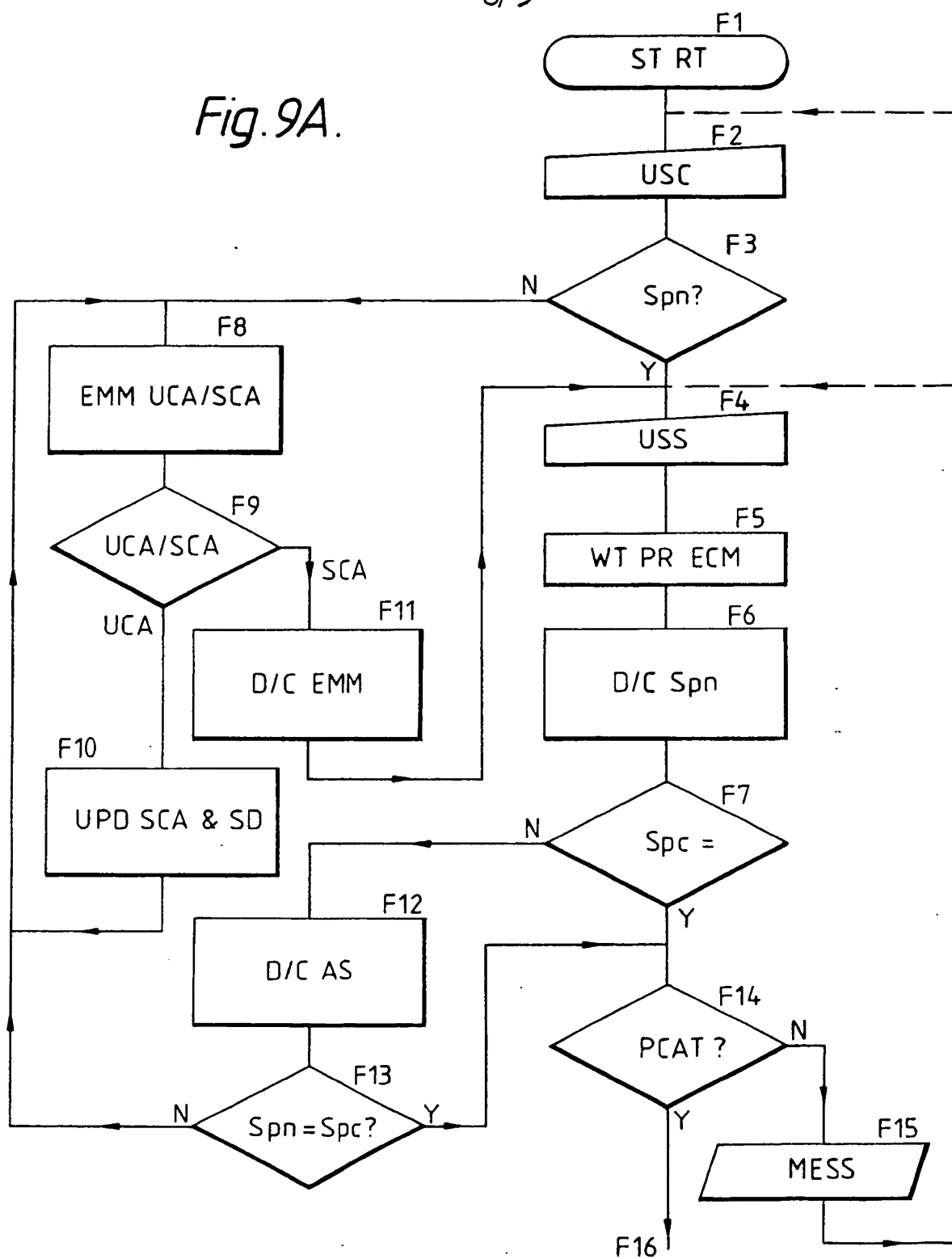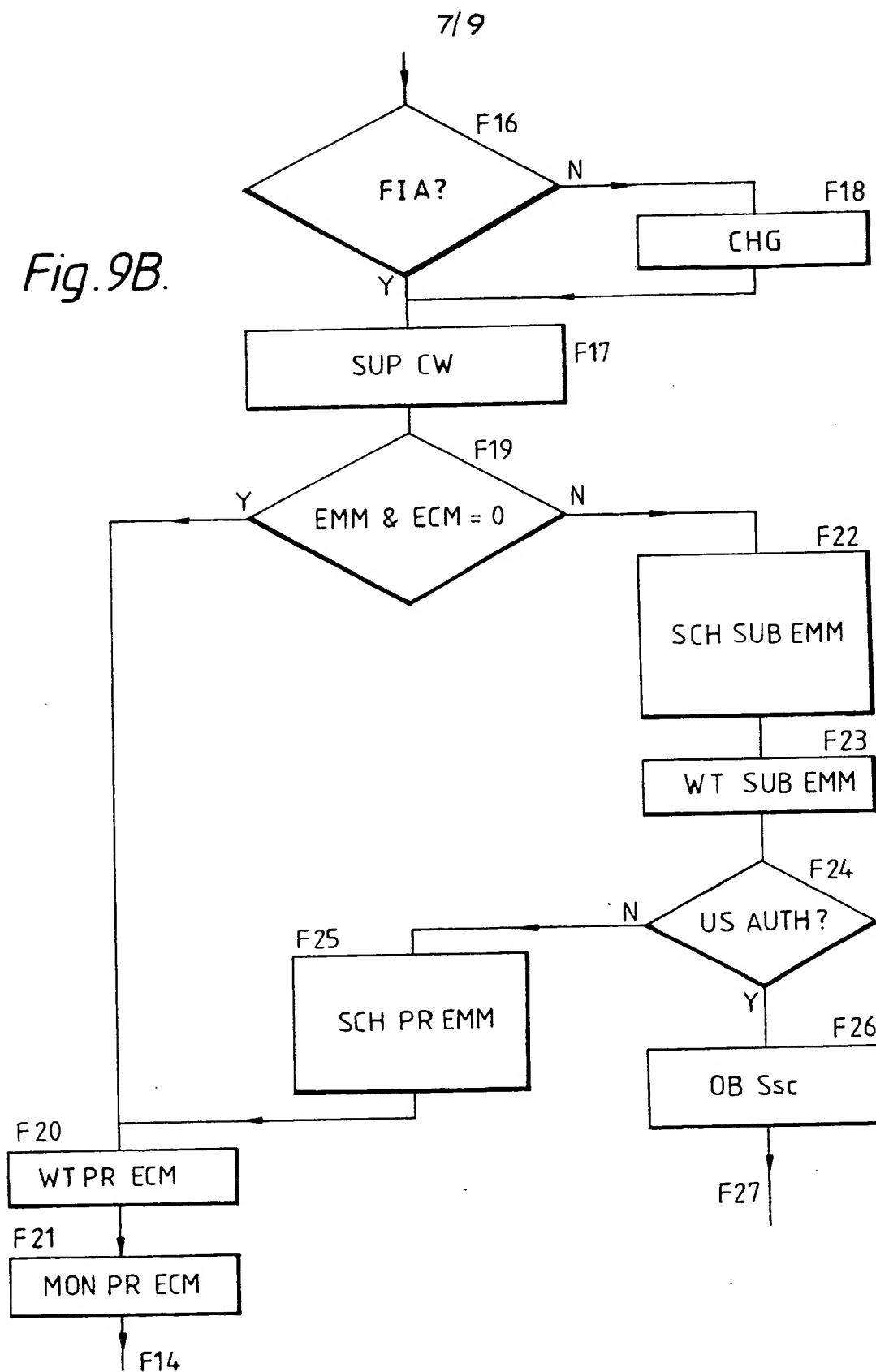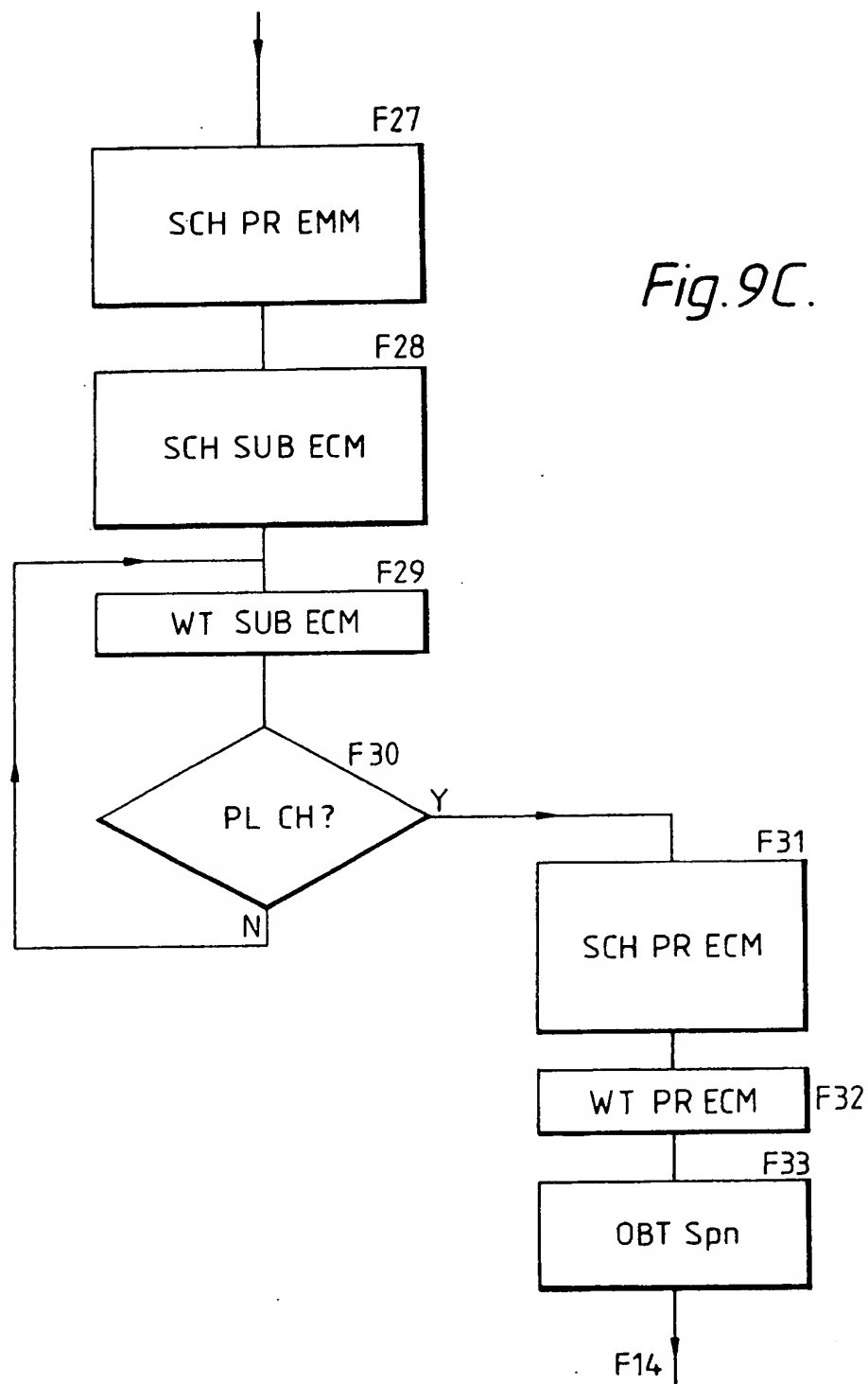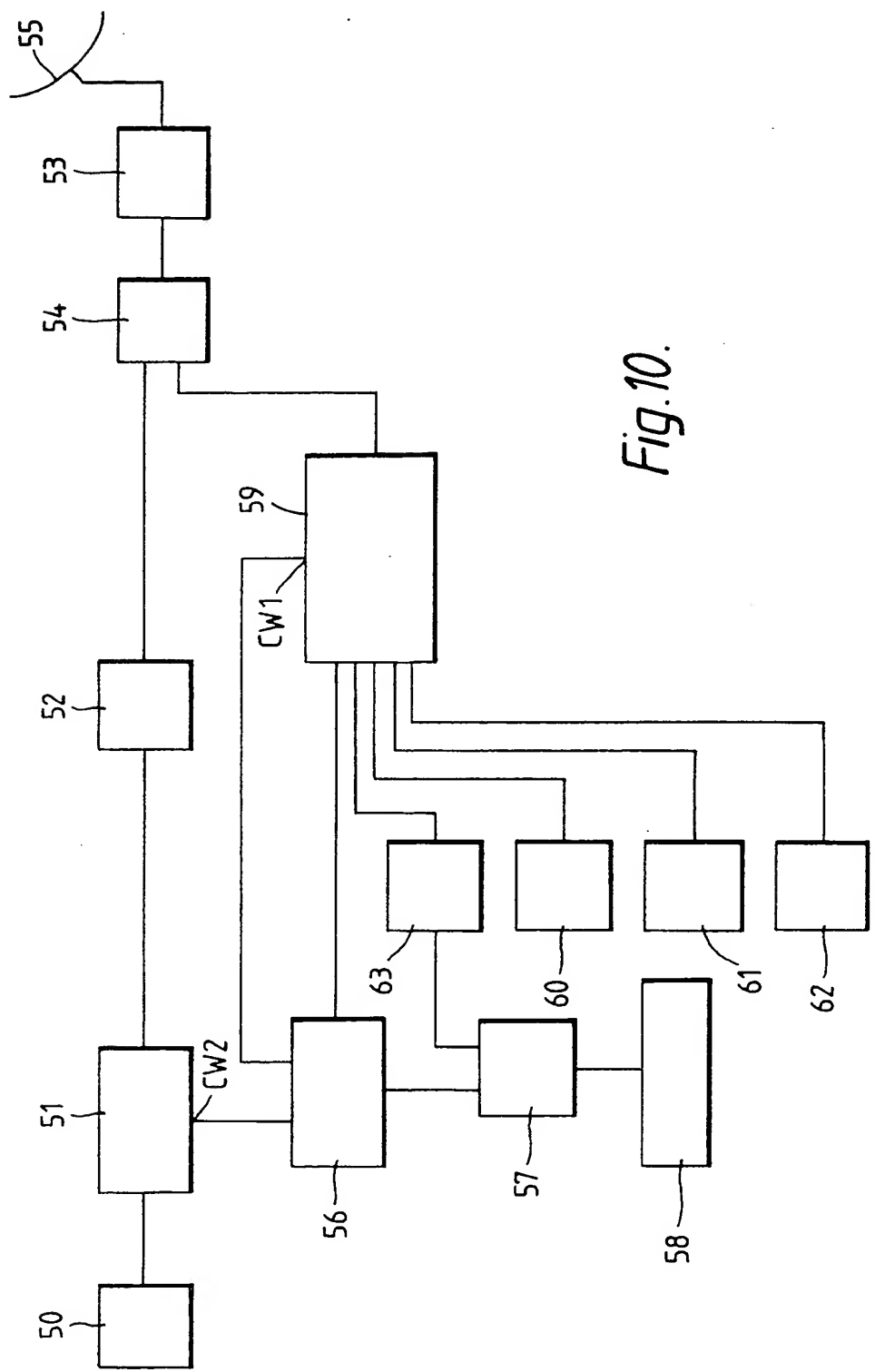
Fig.10.

SPECIFICATION

Decoding transmitting scrambled signals

5 This invention relates to a system for enabling a receiver to decode a transmitted scrambled signal which relates to a programme such that said programme may be obtained in an intelligible manner. The invention also relates to a
10 receiver and a signal generator for use with the system.

A number of proposals have previously been made for authorising subscribers or subscribers' receivers to receive scrambled sig-
15 nals in an intelligible manner. Proposals for over-air addressing are contained in European Broadcasting Union (EBU) documents SPB 284, "Television Standards for the Broadcasting Satellite Specification of the C-MAC Packet
20 System", 3rd revised edition of December 1984, SPB 352, "Methods of Conveying C-MAC/Packet Signals in Small and Large Community Antenna and Cable Networks Installation", also of December 1984, and Doc. JIWP
25 10-11/3-1 of March 1986, which documents are incorporated herein by way of reference. These documents refer to a system, known as System B, which is a shared key over-air addressing system where the scrambling pro-
30 cess i.e. the process that renders the picture and/or sound/data unintelligible, is derived from a truly random control word (CW1 or CW2). The control word and any programme data (P) are encrypted using a supplementary
35 key (S) and the resulting cryptogram S(P,CW) is sent over-air in an Entitlement Checking Message (ECM). The Supplementary key(s) together with customer messages or authorisations (M) are further encrypted using a shared
40 distribution key (D) and the resulting cryptogram D(M,S) is sent over-air an Entitlement Management Message (EMM). The shared distribution key is stored within the viewer's conditional access sub-system (CASS) which en-
45 ables this sub-system to derive the Control Word or words, and to store any authorisations. The EMM has two data streams of which the Unique Customer packets are used to update the CASS in terms of shared distri-
50 bution key, address, etc. and the Shared Customer packets contain the actual entitlements or authorisations.

The above System B proposal is designed to operate at any one time in one mode,
55 either a subscription mode or a pay-per-view mode. The subscription mode is for general or prepaid services where a subscriber is pre-authorised to receive certain or all programmes in an intelligible manner. The pay-
60 per-view mode allows subscribers to select on impulse those programmes they want to receiver the cost for which is deducted from tokens stored in the CASS. As a result of this if a transmission is operating in the subscrip-
65 tion mode and a subscriber is not authorised

to receive the programme of that transmission as it may not be in a class (tier) of programmes he has not requested there is no way in which he can receive that programme
70 in an intelligible manner.

It is an object of the present invention to overcome the above drawbacks.

The invention provides a system for enabling a receiver to decode a transmitted
75 scrambled signal which relates to a programme such that said programme may be obtained in an intelligible manner, wherein in addition to the scrambled signal there are additionally transmitted a subscription key and a
80 pay-per-view key, the receiver functioning in a subscription mode in the event that the receiver is pre-authorised to obtain the programme in an intelligible manner with the scrambled signal being decoded under the
85 control of the subscription key in the presence of an authorising code for the receiver whilst in the absence of such pre-authorisation the receiver is set to function in a pay-per-view mode in which case the programme, on re-
90 quest, is obtained in an intelligible manner with the scrambled signal being decoded under the control of the pay-per-view key.

The advantage of the above system is that it allows receivers to operate in the subscrip-
95 tion mode or in the pay-per-view mode for a given programme. Thus if a subscriber is not authorised to receive this programme in the subscription mode he is not prevented from receiving the programme as he can instead
100 receive the programme in an intelligible manner in the pay-per-view mode. Whilst subscription may be seen as an important method of achieving pay television it is essential that a viewer should always be able to purchase a
105 programme on impulse. This can be achieved with the present invention.

As a delay may exist between the selection of a channel carrying the said programme and the receipt of the appropriate authorising code
110 such that in the event that the receiver is to function in the subscription mode the programme would not be received in an intelligible manner for the period of the delay, the receiver may be capable of being optionally
115 set to function in the pay-per-view mode during the period of the delay to receive the programme in an intelligible manner whereafter the receiver may revert to function in the subscription mode once the appropriate authoris-
120 ing code has been received. This allows the viewer to receive the programme intelligibly if he is not prepared to wait for the authorising code to be received.

On the selection of a channel carrying the
125 said programme the receiver may be automatically set to function in the pay-per-view mode to provide during an initial period the programme in an intelligible manner, which initial period is at least equal to the maximum delay
130 period between said selection and the receipt

of an appropriate authorising code for a pre-authorised receiver. This overcomes the difficulty of the programme being unintelligible until receipt the authorising code appropriate to
5 the receiver at that time.

By or at the end of this initial period the receiver may be set to function in the subscription mode if the receiver is pre-authorised to receive the programme in an intelligible
10 manner but if not so pre-authorised the receiver will continue to function in the pay-per-view mode and only decode the scrambled signal if requested. Thus at the end of this initial period the viewer can have the choice of
15 receiving the programme in an intelligible manner on request or discard the programme.

The subcription key may have a relatively short duration with a given subscription key pertaining to a given programme whilst the
20 pay-per-view key may be of longer duration and pertains to a number of consecutive programmes. In theory the duration of pay-per-view key could lie between 1 hour and 4 months but would typically be between 2
25 weeks and 1 month.

The invention also provides a receiver for use with the above system which comprises means for receiving a scrambled signal relating to a programme, means for receiving a sub-
30 scription key, means for receiving a pay-per-view key, means for receiving authorising codes, means for descrambling said scrambled signal to provide said programme in an intelligible manner, and descrambling control means
35 for controlling the operation of said decrambling means, said receiver functioning in a subscription mode in the event that the descrambling control means receives an authorising code appropriate to the receiver which co-
40 nfirms that the receiver is pre-authorised to obtain the programme in an intelligible manner whereby the scrambled signal is descrambled under the control of said subscription key, whilst in the absence of an authorising code
45 relevant to the said receiver it is set to function in a pay-per-view mode in which case the scrambled signal is descrambled, on request, under the control of the pay-per-view key.

In the event of a delay existing between the
50 selection of a channel carrying the said programme and the appropriate authorising code being received whereby said programme is not produced in an intelligible manner for the period of said delay, the receiver may further
55 comprise means for optionally setting the receiver to function in the pay-per-view mode on request during the delay period whereafter the receiver reverts to function in the subscription mode once the appropriate authoris-
60 ing code has been received.

Means may be provided for automatically setting the receiver to function in the pay-per-view mode on the selection of a channel carrying the said programme to provide during an
65 initial period the programme in an intelligible

manner, which initial period is at least equal to a maximum delay period between the said selection and the receipt of the appropriate authorising code. In such a case means may be
70 provided for setting the receiver to function in the subscription mode at the end of said initial period in the event that the appropriate authorising code is received, said receiver continuing to function in the pay-per-view mode,
75 if required, in the event that the appropriate authorising code is not received.

The invention additionally provides a signal generator for use with the above system which comprises means for providing a signal
80 relating to a programme, means for scrambling the signal, scrambling control means for controlling the operation of said scrambling means, means for generating authorisation keys for authorising selected subscribers to
85 receive said programme in an intelligible manner, means for generating a subscription key and means for generating a pay-per-view key, and means for assembling the authorisation codes, the subscription key and the pay-per-
90 view key with the signal relating to the said programme.

If the subscription key is of short duration means may be provided in the signal generator for producing a different subscription key
95 with each programme.

The above and other features of the invention will now be described, by way of example, in relation to the accompanying drawings in which:
100 Figure 1 is an idealised block diagram of a shared key over-air addressing system used with the present invention,

Figure 2 shows a primary unique customer entitlement management message packet for
105 use with the present invention,

Figure 3 shows a primary shared customer entitlement management message packet for use with the present invention,

Figure 4 shows a primary entitlement check-
110 ing message packet for use with the present invention,

Figure 5 shows the format of a control word command for use with the present invention,
115 Figure 6 shows a subscription shared customer packet for use with the present invention,

Figure 7 shows a subscription entitlement checking message packet for use with the
120 present invention,

Figure 8 is a block diagram of a receiver for use with the present invention,

Figures 9A, B and C shows a flow chart of a program for controlling the operation of a
125 controlled access sub-system for the receiver of Figure 8, and

Figure 10 is a block diagram of a transmitter for use with the present invention.

The system of the present invention is
130 based on the proposal for the System B ac-

cess control system the practical implementation for which is described on page 435 etc. of EBU document SPB 284, on page 206 etc. of EBU document SPB 352 and page 221 etc.
5 of EBU Doc. JIWP 10-11/3-1 mentioned above. A detailed description to System B is not given herein and the reader is directed to the above mentioned documents for an understanding of System B. In the following de-
10 scription the references used in relation to packets and blocks of data and their format are assumed to be as disclosed in the above documents and detailed explanations will only be entered into where these differ from the
15 disclosures.

With the System B proposal the Shared Customer Address (SCA) provides either the subscriber validation or authorisation in the subscription mode or loads tokens into the
20 subscriber's controlled access sub-system in the pay-per-view mode. For a given programme it is not possible for different subscribers to gain entitlement to receive that programme in an intelligible manner by the two
25 different modes nor for a subscriber not pre-authorised to receive that programme to gain access to it via the pay-per-view mode. With the present system both possibilities exist.

Figure 1 shows the shared-key over-air ad-
30 dressing system for System B which is based on Figure 3 of the mentioned parts of the above documents. The figure is divided into three portions where reference 1 denotes the parts contained on the transmission side, ref-
35 erence 2 a transmission path and 3 the parts contained on the receiver side which includes the controlled access sub-system. On the transmission side control words CW (which includes the control words CW1 and CW2)
40 are applied via a connection 4 to a scrambling sequence generator (not shown) to control the scrambling of programme material, both sound and vision. The control word CW is also applied to a first encrypter 5 together with any
45 programme data P and which is encrypted using a supplementary key S to produce at the output of encrypter 5 the cryptogram S(P,CW). The supplementary key S together with customer messages M are applied to a
50 second encrypter 6 and which are encrypted using a shared distribution key D to produce at the output of encrypter 6 the cryptogram D(M,S). In the transmission path 2 the cryptogram S(P, CW) is conveyed in an entitlement
55 checking message (ECM) whilst the cryptogram D(M,S) is conveyed in an entitlement management message (EMM). At the receiver side 3 a first decrypter 7 present in a security device 8 (receives the cryptogram D(M,S) from
60 the EMM together with the shared distribution key D, the decrypter 7 producing the supplementary key S and any customer messages M at separate outputs. A second decrypter 9 receives the cryptogram S(P, CW) from the
65 ECM together with the supplementary key S

from decrypter 7 to produce at separate outputs the control word CW and any programme data P. The control word CW (which again includes the control words CW1 and
70 CW2) is applied via a connection 10 to a descrambling sequence generator (not shown) to control the descrambling of the programme material. The customer message M and the programme data P from the respective outputs
75 of decrypters 7 and 9 are applied to a store 11 for example, for charging purposes.

With the present system two overall encryption channels can be defined, these being a Primary Encryption Channel and a Subscrip-
80 tion Encryption Channel. The Primary Encryption channel is the data path used by the controlled access sub-system to obtain programmes in the pay-per-view mode and it can also be used during switch-on to gain quick
85 access to a service and hence quickly receive a programme in an intelligible manner. This channel in operation is similar to that of System B in the pay-per-view mode except that in the present system token updates are sent
90 using the Unique Customer Packets. The Primary Encryption channel consists of a number of components in packet form. In the following description of various packets each packet contains a packet header (PH) block of 23 bits
95 and a packet type (PT) block of 8 bits which have been omitted from the descriptions although shown in the corresponding figures. In these figures the plain text messages are assembled least significant bit first, encrypted,
100 and then transmitted least significant bit first. Where a number is shown in brackets this indicates the number of bits used for each function, before encryption and error protection (which is not shown).
105 The Primary Encryption channel comprises a Primary EMM and Primary ECM's (one for each separately scrambled service). The Primary EMM comprises Unique Customer and Shared Customer packets. The Unique Cus-
110 tomer packet is shown in Figure 2 and comprises:
UCA Unique customer address as System B—(36) bits.
UCBMD Mode as System B—(4) bits.
115 U Unique Key as System B—(64) bits.
SDKUP Shared distribution key update as System B—(64) bits.
SAUP Shared Address Update as System B—(48) bits.
120 CPUP Customer word position update. The function definition remains the same as System B. The available customer bits have been reallocated to indicate one of 276 customers—(10) bits.
125 CTUP Customer token update. The definition is identical to that given in System B under shared customer packet data format—(12) bits.
Unused—(118) bits.
130 Unallocated—(4) bits.

The blocks UCBMD upto and including the un-
used block of (118) bits are encrypted with
the Unique Key U.

The Shared Customer Packet is shown in
5 Figure 3 and comprises:
SCA Shared customer address—(24) bits.
VALMD Mode. If all bits are set to zero the
operation is as described in this proposal.
Other combinations are reserved for future
10 use—(4) bits.
Spn Next pay-per-view view supplementary
key. Its use and operation are identical to that
in System B except it is only employed with
the primary pay-per-view ECM—(56) bits.
15 Unallocated—(276) bits.
The blocks VALMD and Spn together with the
unallocated block of (276) bits are encrypted
with the Shared Distribution Key D.

The construction of each Primary ECM is
20 shown in Figure 4 and comprises:
CI Command identifier as System B—(8) bits.
LI Length indicator as System B—(8) bits.
PI Parameter identifier whose function is the
same as for System B—(8) bits. Code 00
25 signifies 'pay-per-view' plain text message.
LI Length indicator as System B—(8) bits.
SKL Supplementary key link as System
B—(12) bits.
PASEMM Packet Address for the Subscription
30 shared customer EMM.

This is sent in plain text and allows the
controlled access sub-system to gain access
to the Subscription EMM packets. The two
most significant bits are set to zero. If the
35 packet address given is all zeroes the pro-
gramme being transmitted is solely pay-per-
view and no subscription EMM packets are
being transmitted—(12) bits.
PASECM Packet Address for the Subscription
40 ECM. This again is sent in plain text and al-
lows the controlled access sub-system to gain
access to the Subscription ECM packets. The
two most significant bits are set to zero. If
the packet address given is all zeros the pro-
45 gramme being transmitted is solely pay-per-
view and no subscription ECM packets are be-
ing transmitted—(12) bits.
Spn (Spc) Current pay-per-view supplementary
key encrypted by the next pay-per-view sup-
50 plementary key and has an identical function
to Sn(Sc) in System B—(64) bits.
PI Parameter identifier whose function is the
same as that in System B—(8) bits. Code 02
signifies pay-per-view per unit time as System
55 B whilst code 03 signifies pay-per-view per
programme as System B.
LI Length indicator as System B—(8) bits.
Spc Current primary supplementary key which
has an identical function to Sc in System
60 B—(56) bits.
CW Control word (64) bits. This function tran-
sports even and odd controls words which
can have suffixes from 0 to 7. The even/odd
identification signifies the parity of the condi-
65 tional access frame count thus linking a con-

trol word with an 'odd' or 'even' 256 t.v.
frame period. Figure 5 shows the format of
the CW commmand with the least significant
bit first. In the enlarged section of the first
70 four bits of byte 1 B0, B1 and B2 are the CW
identifier whilst B3 is the least significant bit
of the controlled access frame count to which
the control word corresponds.
PCAT Programme category as System B—(8)
75 bits.
CHID Channel identification as System
B—(169) bits.
PNUM Programme number as System B—(24)
bits.
80 PI Parameter identifier—(8) bits. The block re-
plicates that following Spn(Spc).
PPVPR Pay-per-view price—(24) bits. As Sys-
tem B except PI=02,03, respectively for the
two modes of pay-per-view. That is per unit
85 time or per programme.

5 bytes unallocated—40 bits.
The blocks Spc up to and including PPVPR are
encrypted with Spc.

As far as subscriber authorisation is con-
90 cerned a 'central computer' at the transmis-
sion end will have continous record of the
entitlements of each viewer with respect to
the programmes he is allowed to watch. This
should be the only place where that data is
95 stored and only that data which tells the re-
ceiver that it is (or is not) entitled to receive a
particular programme in an intelligible manner
should be transmitted over-air. This means
that the entitlement authorisations have to be
100 sent out with each programme and that the
subscription supplementary key will only have
a current value (Ssc) changing with every pro-
gramme. To transport the subscription entitle-
ments and the current subscription supplemen-
105 tary key (Ssc) a shared customer EMM em-
ploying 276 by 1 bit authorisations is used.
This EMM can enable (or disable) 20 million or
more viewers in less than 3 minutes using an
effective data capacity of one NICAM Parity
110 mono sound channel whereas with the System
B proposal it would take about 30 minutes to
authorise the same number of viewers. The
subscription Encryption channel contains a
shared customer EMM and the Subscription
115 ECM.

The Subscription shared customer EMM is
shown in Figure 6 and contains
SCA Shared Customer address—(24) bits.
Common to 276 subscribers.
120 VALMD Mode—(4) bits. All bits set to zero
represents the operation as described in this
proposal. Other values are reserved for future
use.
Ssc Current subscription supplementary
125 key—(56) bits.

Definition is similar to that in System B ex-
cept it is employed in conjunction with the
Subscription ECM (see below), and is changed
at the start of each programme.
130 CA Customer Authorisations. 276 × 1 bit

customer authorisations used to enable a customer and allow the controlled access subsystem to gain access to the subscription ECM and hence the control words. A binary
5 '1' corresponds to being enabled.
The blocks VALMD, Ssc and CA are encrypted with the Shared Distribution Key D. This method of customer authorisation is dealt with in greater detail in published European
10 Patent Application No. 0 132 007 A1. As proposed here it allows 20×10^6 or more viewers to be authorised in less than 3 minutes. The current subscription supplementary key Ssc is changed at the end of each pro-
15 gramme to avoid piracy as it could be envisaged that a subscriber could take out a minimum subscription and be validated quite legally and still get access to the Ssc if this were long term. The subscriber could then in-
20 struct his receiver to ignore all further subscription shared customer EMM's and although his location (authorisation) bit may be switched to disable the receiver will continue to receive valid programmes until the Ssc is
25 changed. Thus, if for a sequence of programmes a new Ssc is required for each programme and re-validation required for each programme.
The Subscription ECM is shown in Figure 7
30 and contains:
CI Command identifier as System B—(8) bits.
LI Length indicator as System B—(8) bits.
PI Parameter identifier whose function is the same as for System B—(8) bits. Code 01
35 signifies 'subscription' plain text message.
LI Length indicator as System B—(8) bits.
PL Programme Link—(16) bits. This give advanced indication of a change in Ssc, i.e. at the end of programme. The 16 bits corre-
40 spond to the 16 least significant bits of the controlled access frame count.
PI Parameter identifier whose function is the same as for System B—(8) bits. Code 04 'subscription' cipher text message.
45 LI Length indicator as System B—(8) bits.
Ssc Current Subscription Supplementary key—(56) bits.
Definition is similar to that in System B and is used here as a security check. CW, PCAT,
50 CHID, PNUM, PI as defined in the Primary ECM (Figure 4).
30 bytes unallocated—240 bits.
The blocks Ssc up to and including PI are encrypted with Ssc.
55 Whilst by using a system of packets as described above to achieve the ability of receiving a programme either in the subscription or pay-per-view modes, it also offers a high degree of security. The security aspects are
60 based on the following:
i. The security of the system is based on the Unique address, the Unique key and if these are tied to a specific brand and serial number of receiver the security is further en-
65 hanced.

ii. Cloning of the system must be one approach of a pirate to avoid payments. However, if the checks set out in (i) above are strictly applied then programme purchase
70 would have to be by a single person and the unit a major item. Cloning is only of advantage in the subscription mode, it does not give free pay-per-view. Further the system allows for a Unique address to be disabled from the sys-
75 tem by giving a new shared address to the other 275 valid occupants of that address. The old shared address is no longer transmitted and up-dated with the new keys. No legally purchased systems are disabled.
80 iii. Another level of attack has to be at the shared address packet and its contents. In particular the next supplementary key Spn. If in some way access could be achieved to this key then it could be envisaged that the pay-
85 per-view mechanism could be by-passed. To reduce the risk of this occurring important keys such as Spn which have to be stored in the control access unit for significant periods could be stored encrypted with the Unit's Uni-
90 que key. In this way the plain text version of these keys only exist transiently in the control access sub-system central processor unit. Considerable care should be given to the security of the Unique address key.
95 iv. In the subscription mode the keys are of short duration.
However, a possible method of attack is to arrange that all the customer bits are set to enable. It seems extremely unlikely that this
100 could be done on the received signal and would have to be tackled within the controlled access sub-system software.
v. A controlled access sub-system designed to by-pass the above with a Unique address
105 and key from a legitimately purchased unit could be envisaged. Such an item would be more difficult to detect since it would only be necessary to apply for a shared address once. However, if the legitimate industry does not
110 provide an interface for such a unit then the pirate is still faced with the marketing problems identified under (ii) above.
A receiver using the present system is shown in Figure 8 for receiving signals from a
115 C-MAC transmission and where the reference 12 indicates a dish aerial suitable for receiving satellite television signals in the 12GHz band, the aerial having a down converter 13 attached to it which frequency converts the in-
120 coming television signal to a frequency within the 1 to 2GHz band depending of course on the frequency of the incoming signal. The down converted signal is applied over a co-axial cable 14 to a terminal 15 forming the
125 input for the television receiver, this terminal 15 being connected to an r.f. amplifier and frequency changer stage 16 which amplifies and transforms the incoming signal to a suitable i.f. frequency of about 480MHz which is
130 further amplified by an i.f. amplifier 17. The

output of the amplifier 17 is applied to a fre-
quency demodulator 18 as the vision compo-
nents of the broadcast satellite television sig-
nal are frequency modulated, the demodulated
5 output of the demodulator 18 being applied to
an input of a MAC signal analogue processor
unit 19 which separates the analogue vision
components from the MAC signal. The output
of the i.f. amplifier 17 is also applied to a
10 digital demodulator stage 20 where the incom-
ing digital signals which are 2-4 PSK modu-
lated are converted to normal binary form and
from which synchronising information and vari-
ous clock frequencies are derived together
15 with the sound/data and control signals and
applied to the analogue processor unit 19.
The vision components from the analogue
processor unit 19 are applied to an analog to
digital converter 21 for conversion to digital
20 form and thence applied to a vision decoder
22 where the luminance and chrominance vi-
sion components, subjected to line cut rota-
tion scrambling at the transmission source, are
descrambled and re-assembled for application
25 to a digital to analog converter 23 to produce
simultaneous analogue Y, U and V compo-
nents for application to a matrix (not shown)
prior to being prepared for display.
The data and clock signals from the digital
30 portion of the MAC signal are applied from
the analogue processor unit 19 over a connec-
tion 24 to a sync. control unit 25 where vari-
ous data and synchronising information are
processed under the control of a microproces-
35 sor 26. Such data are contained in certain
areas of the multiplex such as the Service In-
formation (SI) packets and data in line 625
and are applied to the microprocessor 26 over
a connection 27. Control data for the sync.
40 control unit 25 is applied from the micropro-
cessor 26 over a connection 28. The sync.
control unit 25 applies control data over a
connection 29 to the analogue processor unit
19 to control the timing of the digital data to
45 unit 25 and the analogue signals to converter
21 whilst a connection 30 applies control data
to the vision decoder 22 to control the des-
crambling and assembly of the Y, U and V
components of the vision signal. The latter
50 control data will include the control word
CW2 for application to a descrambling se-
quence generator controlling the descrambling
of the vision components. Data and control
signals, including the control word CW1 for
55 application to a descrambling of the sound/-
data components, are applied over a connec-
tion 31 to a sound decoder 32 where the
appropriate sound/data services are selected
and descrambled, the sound/data signals hav-
60 ing been subjected to scrambling at the
transmission source by the addition of a
pseudo random sequence using an exclusive
OR-gate. The appropriate descrambled sound/-
data services are applied from the sound de-
65 coder 32 to a second digital to analog conver-

ter 33 to produce (say) two such services S1,
S2 for reproduction.
The microprocessor 26 is additionally con-
nected over a two way connection 34 to an
70 interface 35 conveying the data needed for
communication with a controlled access sub-
system 36 which is connected by input (37)
and output (38) connections. The components
of the sub-system 36 may be contained
75 within the receiver or may be present on a
SMARTCARD or other such similar device as
already proposed and connected to the re-
ceiver as required. The sub-system 36 con-
tains an interface 39 between the input and
80 output connections 37, 38 and a bus 40. The
bus 40 interconnects a central processor unit
41 with a read only-memory (ROM) 42 which
provides the program for running the sub-sys-
tem, a random access memory (RAM) 43
85 which stores data, and a non-volatile memory
(NVM) 44 which provides long time storage
for long term keys such as the Unique key
and the Supplementary keys. It is the con-
trolled access sub-system 36 in combination
90 with the other parts of the receiver which
controls which services may be received in an
intelligible manner and the control software of
the sub-system 36 is organised to that end.
The flow chart of Figures 9A, 9B and 9C
95 provides an illustration of such control soft-
ware.
In the flow chart of Figures 9A, 9B and 9C
the various boxes and the legends contained
therein specify the control software steps as
100 fo11ows:
F1: STRT This is an instruction to enter the
program.
F2: USC At this point the user selects the
channel he wishes to receive.
105 F3: Spn? This is an instruction to determine
whether a next pay-per-view supplementary
key (Spn) value is present in the non-volatile
memory 44.
F4: USS At this point the user selects the
110 service in the channel he wishes to receive.
The access related message (ACCM) in packet
'0' supplies the decoder with the appropriate
ECM packet address.
F5: WT PR ECM This is an instruction to wait
115 for the primary ECM packet.
F6: D/C Spn This is an instruction to attempt
to decrypt the primary ECM assuming that the
stored Spn equals the actual Spn by first deci-
phering Spn(Spc).
120 F7: Spc = This is an instruction to determine
whether Spc from Spn(spc) equals Spc from
the ciphertext block.
F8: EMM UCA/SCA This step is entered into
when step F3 does not find an Spn value in
125 NVM 44 and is an instruction to wait for a
primary EMM having a packet address given
by List X in packet '0', with either a Unique
customer address (UCA) or shared customer
address (SCA) (if known). This step is also
130 entered into on two other conditions (below).

F9: UCA/SCA? This is an instruction to determine whether an UCA or an SCA is present.

F10: UPD SCA & Sd This is an instruction, if an UCA is present at step F9 to update the
5 SCA and the shared distribution key (SD) (and tokens). Once this instruction is completed the program reverts to step F8.

F11: D/C EMM This step is entered into if an SCA is present at step F9 and is an instruc-
10 tion to decipher the EMM to get the next pay-per-view supplementary key (Spn) and to store it in the NVM 44.

F12: D/C AS This step is entered into if Spc from Spn(Spc) does not equal Spc from
15 ciphertext block at step F7 and is an instruction to attempt to decrypt assuming that the stored Spn is equal to the actual Spc.

F13: Spn=Spc? This is an instruction to determine whether the stored Spn (used for de-
20 crypting) equals Spc from the ciphertext block. If these are not equal the program reverts to step F8.

F14: PCAT? This is an instruction to determine whether the programme category (PCAT)
25 permits access to this service.

F15: MESS This is an instruction to display an explanatory message if PCAT at step F14 does not permit access.

F16: FIA? This is an instruction to deterine
30 whether the user is entitled to free instant access to the service (user may have done this within the last (say) 15 minutes).

F17: SUP CW This is an instruction to the decoder to be supplied with control words
35 CW.

F18: CHG This step is entered into if at step F16 the user is not entitled to free instant access and is an instruction to commence charging at the normal pay-per-view rate.
40 F19: EMM & ECM = 0? This is an instruction to determine whether the subscription EMM and ECM addresses in the primary ECM packet are both zero.

F20: WT PR ECM This step is entered into if
45 step F19 determines that the Subscription EMM and ECM addresses in the primary ECM packet are both zero and is an instruction to wait for the primary ECM packet. The status quo has now been achieved with user charged
50 as pay-per-view.

F21: MON PR ECM This is an instruction to monitor the primary ECM's for a change in programme number (PNUM) and on a change of PNUM to go to step F14.
55 F22: SCH SUB EMM This step is entered into if step F19 determines that the subscription EMM and ECM addreses in the primary ECM packet are not both zero and is an instruction for the decoder to search for subscription
60 EMM packets with addresses from primary EMM packets. F23: WT SUB EMM This is an instruction to wait for subscription EMM packet.

F24: US AUTH: This is an instruction to the
65 decoder to decipher the subscription EMM to

determine whether the user is authorised.

F25: SCH PR EMM This step is entered into if step F24 determines the user is not authorised and is an instruction to the decoder to
70 search for primary EMM packets again instead of subscription EMM packets. When found goes to step F20.

F26: OBT Ssc This step is entered into if step F24 determines that the user is authorised
75 and is an instruction to obtain the current subscription supplementary key Ssc.

F27: SCH PR EMM This is an instruction for the decoder to search for primary EMM packets again instead of subscription EMM pack-
80 ets.

F28: SCH SUB ECM This is an instruction for the decoder to search for subscription ECM packets rather than primary ECM packets.

F29: WT SUB ECM This is an instruction to
85 wait for subscription ECM packet.

F30: PL CH? This is an instruction to the decoder to decipher the subscription ECM packet to determine whether the Programme Link (PL) in subscription ECM packets indicates an im-
90 minent change of Ssc. If no such change is indicated the program cycles through steps F29 and F30.

The status quo has been acheived with the user receiving a service to which he has sub-
95 scribed, but PL continued to be monitored to anticipate a change of Ssc and hence the end of the programme.

F31: SCH PR ECM This step is entered into if step F30 determines that PL does indicate an
100 imminent change of Ssc meaning that the end of the programme is imminent and is an instruction to the decoder to search for primary ECM packets again rather than subscription ECM packets.
105 F32: WT PR ECM This is an instruction to wait for primary ECM packet.

F33: OBT Spc This is an instruction to decrypt the primary ECM by first using the stored Spn to obtain Spc from Spn(Spc) and
110 then return to step F14.

The strategy of the above software is to always engage the Primary mode (pay-per-view) before establishing the subscription mode. This ensures that normal viewing will
115 always be obtained with mininal delay, due to the longer term pay-per-view supplementary key (Spc). The cover-time of this key may be 2-3 weeks which means that the controlled access sub-system will usually have the key
120 stored in its memory from a previous viewing session either in its 'next' or 'current' form.

In this way 'free viewing' can be given during a switch on phase whilst the controlled access sub-system searches for the subscrip-
125 tion authorisation. This free viewing period works in the following way. Although other methods could be used, it is believed that the one described is adequate to deter most forms of piracy. Each programme has a unique
130 identification given to it by the channel identifi-

cation (CHID) and programme number (PNUM) sent in the ECM data streams. Thus every programme that has been accessed by the controlled access sub-system can be recorded

5 in its memory (this information could also be used for market research, etc.) To prevent a viewer from obtaining successive free viewing periods, by either turning his 'set' on and off, or changing channel and returning, the con-

10 trolled access sub-system compares the current identification with those stored over say the last 15 minutes and if any match the controlled access sub-system starts to charge at the pay-per-view rate.

15 If after the search for subscription authorisation the controlled access sub-system has been enabled by the subscription shared customer EMM, the sub-system then operates in subscription mode mode monitoring the sub-

20 scription ECMs for changes in programme using the programme link (PL). However, if authorisation is not received the user is offered the possibility of staying in pay-per-view mode charged either on a programme or unit time

25 basis. The switching from one encryption channel to another is achieved by commands send by the controlled access sub-system to the decoder hardware by means of the conditional access interface. The relevant packet

30 addresses are obtained from the SI (though the above EBU documents do not, at present, allow the signalling of EMM channels linked to a particular service), or internally derived from the Primary ECM packets.

35 In the flow chart the programme category (PCAT) is used as a 'parental key' further restricting programme access on a local basis, e.g. to prevent young children from watching 'adult material'. Unless authorisation is denied,

40 the access process is totally transparent to the user; only in the pay-per-view mode is the user involved in making a decision.

Figure 10 shows a block diagram of a signal generator for use with the above system, the

45 transmission system used being one of the MAC/Packet family as described in the above EBU documents. For the present it will be assumed that the transmission system is that of C-MAC Packet. In Figure 10 a vision signal

50 source 50 which may be a television camera or a video tape recorder has its output connected to a vision signal processor 51 in which the analogue chrominance and luminance components are converted to digital si-

55 gals, compressed, and scrambled by the "line cut" method before being converted back to analogue signals. The cut will not be at the same place in each line but may be made at one of a possible 256 positions. For this pur-

60 pose the vision processor will also contain a scrambling sequence generator (not shown) which receives the control word CW2 as explained above in relation to Figure 1.

The output from the vision processor 51 is

65 applied to a frequency modulator 52 and the modulated output applied to a suitable transmitter 53 via an adder circuit 54, the transmitter producing a modulated output in the 12GHz band from which it will be applied

70 to a suitable aerial system 55 for transmission to a satellite.

The control word CW2 is generated in a security device 56 which contains the components shown at the transmission side 1 in

75 Figure 1 as well as generators for the supplementary key S and the shared distribution key D. A central computer 57 is connected to the security device 56 and in which is held the details of those subscribers who have made

80 pre-payment for programme authorisation and also includes information as to which programmes subscribers are actually authorised for. A keyboard 58 is connected to the central authorisation computer 57 to enter and

85 modify subscriber authorisation information as is necessary. The security device 56 produces at its output the packets of data shown in Figures 2 to 7 for controlling access to a programme in the subscriber's receivers either in

90 the subscription or pay-per-view modes this output being applied to a first input of a sound/data processor 59. Two sound sources 60 and 61 producing signals in digital form are connected to further inputs of the proces-

95 sor 59 whilst an additional input receives the sync. words W1, W2 from a sync. generator 62. The central computer 57 also contains service information regarding the programmes currently being transmitted and this informa-

100 tion is applied to a service data processor 63 which formats this information into service information data and line 625 data, the output of the service data processor 63 being applied to a further input of the sound/data processor

105 59. The signals applied to the inputs of the processor 59 are formed into packets before being assembled with the sync. words into the data burst. The signals in the data burst are scrambled in the sound/data processor by

110 being added in an exclusive OR-gate with a pseudo random sequence under the control of control word CW1 received from the security device 56. The portion of the data burst which appears in each television line is 2-4

115 PSK modulated and the modulated output from processor 59 is applied to a second input of the adder circuit 54 where it is added with the frequency modulated vision signal.

120 CLAIMS
1. A system for enabling a receiver to decode a transmitted scrambled signal which relates to a programme such that said programme may be obtained in an intelligible

125 manner, wherein in addition to the scrambled signal there are additionally transmitted a subscription key and a pay-per-view key, the receiver functioning in a subscription mode in the event that the receiver is pre-authorised to

130 obtain the programme in an intelligible manner

with the scrambled signal being decoded under the control of the subscription key in the presence of an authorising code for the receiver whilst in the absence of such pre-authorisation the receiver is set to function in a pay-per-view mode in which case the programme, on request, is obtained in an intelligible manner with the scrambled signal being decoded under the control of the pay-per-view key.

2. A system as claimed in Claim 1, in which a delay may exist between the selection of a channel carrying the said programme and the receipt of the appropriate authorising code such that in the event that the receiver is to function in the subscription mode the programme would not be received in an intelligible manner for the period of the delay, the receiver being capable of being optionally set to function in the pay-per-view mode during the period of the delay to receive the programme in an intelligible manner whereafter the receiver reverts to function in the subscription mode once the appropriate authorising code has been received.

3. A system as claimed in Claim 1, in which on the selection of a channel carrying the said programme the receiver is automatically set to function in the pay-per-view mode to provide during an initial period the programme in an intelligible manner, which initial period is at least equal to a maximum delay period between said selection and the receipt of an appropriate authorising code for a pre-authorised receiver.

4. A system as claimed in Claim 3, in which by or at the end of said initial period said receiver is set to function in the subscription mode if the receiver is pre-authorised to receive said programme in an intelligible manner but if not so pre-authorised the receiver will continue to function in the pay-per-view mode and only decoder the scrambled signal if requested.

5. A system as claimed in any of the preceding claims, in which the subscription key has a relatively short duration with a given subscription key pertaining to a given programme whilst the pay-per-view key is of longer duration and pertains to a number of consecutive programmes.

6. A system for enabling a receiver to decode a transmitted scrambled signal substantially as herein described with reference to the accompanying drawings.

7. A receiver for use with a system as claimed in any of the prceding claims, said receiver comprising means for receiving a scrambled signal relating to a programme, means for receiving a subscription key, means for receiving a pay-per-view key, means for receiving authorising codes, means for descrambling said scrambled signal to provide said programme in an intelligible manner, and descrambling control means for controlling the

operation of said descrambling means, said receiver functioning in a subscription mode in the event that the descrambling control means receives an authorising code appropriate to the receiver which confirms that the receiver is pre-authorised to obtain the programme in an intelligible manner whereby the scrambled signal is descrambled under the control of said subscription key, whilst in the absence of an authorising code relevant to the said receiver it is set to function in a pay-per-view mode in which case the scrambled signal is descrambled, on request, under the control × of × the pay-per-view key.

8. A receiver as claimed in Claim 7, in which in the event of a delay existing between the selection of a channel carrying the said programme and the appropriate authorising code being received whereby said programme is not produced in an intelligible manner for the period of said delay, said receiving comprising means for optionally setting the receiver to function in the pay-per-view mode on request during the delay period whereafter the receiver reverts to function in the subscription mode once the appropriate authorising code has been received.

9. A receiver as claimed in Claim 7, in which means are provided for automatically setting said receiver to function in the pay-per-view mode on the selection of a channel carrying the said programme to provide during an initial period the programme in an intelligible manner, which initial period is at least equal to a maximum delay period between the said selection and the receipt of the appropriate authorising code.

10. A receiver as claimed in Claim 9 in which means are provided for setting the receiver to function in the subscription mode at the end of said initial period in the event that the appropriate authorising code is received, said receiver continuing to function in the pay-per-view mode, if requested, in the event that the appropriate authorising code is not received.

11. A receiver substantially as herein described with reference to Figures 1 to 9 of the accompanying drawings.

12. A signal generator for use with a system as claimed in Claims 1 to 6, said signal generator comprising means for providing a signal relating to a programme, means for scrambling said signal, scrambling control means for controlling the operation of said scrambling means, means for generating authorisation codes for authorising selected subscribers to receive said programme in an intelligible manner, means for generating a subscription key and means for generating a pay-per-view key, and means for assembling the authorisation codes, the subscription key and the pay-per-view key with the signal relating to the said programme.

13. A signal generator as claimed in Claim

12, in which said subscription key is of short
duration, said signal generator comprising
means for producing a different subscription
key with each programme.

5　　14. A signal generator substantially as
herein described with reference to Figures 1
to 7 and 10 of the accompanying drawings.